

MOVEIT DMZ: WEB APPLICATION USAGE OF MOVEIT DMZ SERVICES

This document discusses how the MOVEit DMZ secure managed file transfer (MFT) server software by Ipswitch File Transfer can be used as a backend system by Portals and other Web applications, providing them with secure, programmatic access to MOVEit DMZ secure file and message transfer services as well as to its secure data storage, user permissions, and audit trail database services.

PRODUCT OVERVIEW

MOVEit DMZ is a well-regarded and widely-deployed secure MFT server. It is typically located on a firewall-attached network segment known as a “de-militarized zone” (a DMZ, hence its name). MOVEit DMZ is in production use by small, medium, and large companies and government agencies in North America, Europe, and around the Pacific Rim where it is used to securely transfer, store, and control access to consumer, financial, human resource, legal, and medical data as well as to trade secrets and other confidential information.

MOVEit DMZ was designed and developed as a secure MFT solution. It is not an FTP server with grafted-on security features, nor is it a proprietary program with open standards support added-on. Below are just a few examples of the defense-in-depth security that is designed into MOVEit DMZ.

FIPS 140-2 Validated Cryptography, including 256-bit AES storage encryption.

Multi-Factor Authentication support for two or even three factors, including passwords, SSH Public keys (“fingerprints”), IP addresses/address ranges, and SSL software and hardware-based client certificates (including those on CAC cards).

File Integrity Checking using cryptographically-valid SHA1 hashing of all uploaded and downloaded files (required for file Non-Repudiation and Guaranteed Delivery).

End-to-End Encryption using AS2, AS3, secure ftp over SSH2 (SFTP/SCP2), secure FTP over SSL (FTPS/TLS) and secure hypertext transfer protocol (HTTPS) encrypted transport together with MOVEit DMZ’s built-in automated FIPS 140-2 validated 256-bit AES encrypted file storage.

OS Security Independence because MOVEit DMZ has its own built-in secure encrypted file storage system and access control/user permissions system, which means the security of the users, files and messages that MOVEit DMZ handles does not depend on the security (or lack thereof) of the underlying operating system.

Virtual User Interface, which helps implement “least privilege” by providing tight administrative control over what users can and cannot see and do in terms of MOVEit DMZ command options, files, folders, logs and user information.

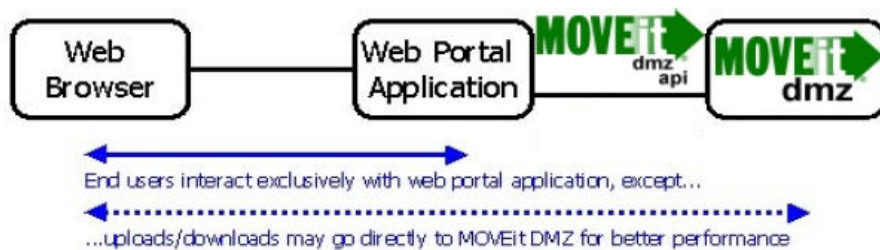
MOVEit DMZ can be used to achieve and demonstrate compliance with corporate, contractual, industry and regulatory privacy and security standards, including GLBA, HIPAA, PCI DSS, MA 201 CMR 17 and SOX.

The MOVEit DMZ software runs as a service on a dedicated Microsoft Windows 2003 host system, which can be either physical or virtual (under either EMC VMware EXS and Microsoft Virtual Server).

WEB APPLICATION ACCESS TO MOVEIT DMZ SERVICES AND DATA

In addition to being deployed as a standalone secure data exchange portal, MOVEit DMZ is also used as a backend system providing Portals and other Web apps with secure file transfer and message services, as well as secure data storage, user permissions, and audit trail database services.

Web applications connect to these services through the MOVEit DMZ API XML machine interface, which provides them with secure, programmatic access to MOVEit DMZ services and related data. Web apps securely connect, authenticate and communicate with the API via a 128-bit SSL encrypted, firewall-friendly HTTPS connection using either a MOVEit DMZ API Java and Windows client.



Note: Providing direct Web application access to MOVEit DMZ secure file transfer and messaging services and data requires modifying the application by either adding or modifying a secure page to present file upload/download and/or secure message creation/sending/receiving options to users.

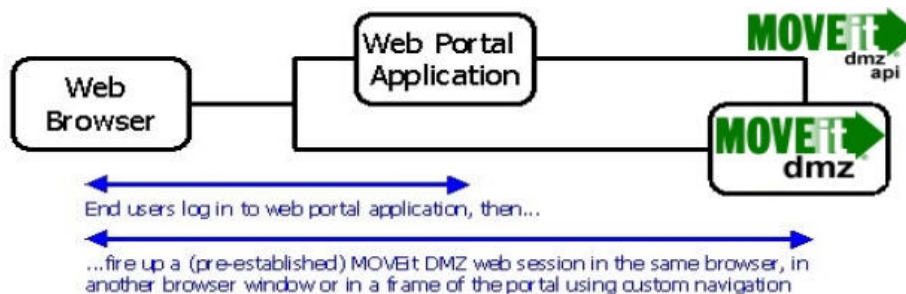
USER ACCESS TO MOVEIT DMZ SERVICES AND DATA

A user logged into a Portal or other Web application can be given direct access to MOVEit DMZ secure file transfer and/or secure messaging services and data using either of the methods below.

Session Transfer. The user's session can be transferred from the app to MOVEit DMZ.

Session Duplication. A second, simultaneous session can be created on MOVEit DMZ.

In both cases the Portal or Web application logs in to MOVEit DMZ using a MOVEit DMZ API client.



SECURE FILE TRANSFER SERVICES

Portals and other Web apps can provide their users with direct or indirect access to MOVEit DMZ secure file transfer services and related data. Those users can be running Firefox, Internet Explorer, Navigator, Netscape,

Opera or Safari browsers — without having to use ActiveX, Java or plugins. MOVEit DMZ provides browser-equipped users with the following advanced file transfer capabilities.

Encrypted File Storage. All files received by MOVEit DMZ are automatically encrypted before being stored. MOVEit DMZ does this using its own strong, built-in, FIPS 140-2 validated 256-bit Advanced Encryption Standard (AES) encryption, which uses a separate key for each file it encrypts, and encrypts each key for true ‘defense in depth’ security. MOVEit DMZ provides end-to-end encrypted file transfer and storage, without needing to buy, distribute or manage keys for third-party encryption programs such as PGP.

Email Notification. MOVEit DMZ can automatically email notices to file senders and/or recipients, alerting them when specific files have been received, viewed, downloaded or deleted, or when a recipient has not viewed a file within a time period set by the sender.

Multi-Lingual Interface Option. Users of MOVEit DMZ’s Web interface can select between English or separately licensed French or Spanish language user interfaces.

Audit Trail. Each user, file and administrative action is automatically recorded to the secure, remotely accessible, tamper-evident, ODBC-accessible MOVEit DMZ database.

While Web browsers have many advantages when used as secure file transfer clients, they lack valuable basic and advanced capabilities. Specific browsers have upload file size limits and/or time-out restrictions that can halt the transfer of large files over slow or unreliable connections. These and other browser limitations can be overcome by using the free MOVEit Wizard plugins, which also provide with the following advanced file transfer capabilities not found in browsers.

Multi-File Transfers. Ability to easily upload multiple files in a single transfer.

Integrity Checking. Using SHA-1 hashing (required for file Non-Repudiation).

Non-Repudiation. The ability to prove who sent a file, who received it, and that the file sent and the file received are exactly the same (required for Guaranteed Delivery).

Guaranteed Delivery. Consisting of file Non-Repudiation, support for transfer retry and resume, automated file arrival email notification, and a detailed audit trail.

Automatic File Compression. Provides faster transfers of compressible files.

Transfer Status Bar. Visual feedback to users on the progress of each file transfer.

Commercial use of the MOVEit DMZ secure file transfer and storage services described on this page, including the unlimited downloading and use of MOVEit Wizard Web browser plugins, are provided for under the product’s Basic license (see page 8 for details). Note: Portals and Web applications must provide direct user access to MOVEit DMZ in order to support MOVEit Wizards.

SECURE MESSAGING SERVICES

Portals and Web applications can utilize MOVEit DMZ Secure Messaging services to enable their users to securely compose, send, store and receive confidential information in an email-like message form, with or without attached files. Messages and attachments are securely transmitted via MOVEit DMZ using 128-bit SSL encryption, and securely stored using its strong, built-in, FIPS 140-2 validated 256-bit AES encryption. (See “FIPS 140-2 Validated Cryptography” on page 8 for details.)

Firefox, Internet Explorer, Navigator, Netscape, Opera and Safari Web browsers can all be used to securely exchange messages via MOVEit DMZ — without having to use ActiveX, Java or plugins. MOVEit DMZ provides browser-equipped users with the following advanced messaging capabilities.

Encrypted File Storage. All messages and file attachments received by MOVEit DMZ are automatically encrypted before being stored. MOVEit DMZ does this using its own strong, built-in, FIPS 140-2 validated 256-bit Advanced Encryption Standard encryption, which uses a separate key for each file it encrypts, and encrypts each key for true ‘defense in depth’ security. MOVEit DMZ provides end-to-end encrypted message and file transfer and storage, without needing third-party encryption programs such as PGP.

Email Notification. MOVEit DMZ can automatically email senders and/or recipients, alerting them when specific messages have been viewed or deleted, attached files downloaded, or when a message has not viewed within a time period set by the sender. (Note: These are the only use of email by the MOVEit DMZ Secure Messaging services.)

Multi-Lingual Interface Option. Users of MOVEit DMZ’s Web interface can select between English or separately licensed French or Spanish language user interfaces.

Audit Trail. Each user, file and administrative action is automatically recorded to the secure, remotely accessible, tamper-evident, ODBC-accessible MOVEit DMZ database.

While secure messaging is an integral part of the MOVEit DMZ codebase, it is a separately licensed and priced option. The secure messaging option permits an unlimited number MOVEit DMZ users to create, exchange and store an unlimited number of messages and attached files. Note: Web applications must provide direct user access to MOVEit DMZ in order to use MOVEit Wizard.

Note: MOVEit Wizards are not required for MOVEit DMZ Secure Messaging, though their use will provide the advanced capabilities listed on page 3 when uploading or downloading file attachments.

SECURE FILE AND MESSAGE STORAGE SERVICES

Portals and Web applications that use MOVEit DMZ secure file transfer and/or messaging services will automatically be using MOVEit DMZ secure storage capabilities, and they can elect to make use of these capabilities to securely store any files that the portal or Web application generates or uses.

Secure data storage can be a very important element of the security of a portal or other Web app because any confidential data it stores unencrypted (in the clear) on an Internet accessible server is vulnerable to being read, modified or deleted by anyone who hacks the server’s operating system.

MOVEit DMZ eliminates this vulnerability by automatically encrypting every file and message it receives -- before storing them to disk. MOVEit DMZ does this using its own strong, built-in, FIPS validated 256-bit Advanced Encryption Standard (AES) encryption, which uses a separate key for each file and message it encrypts (see “FIPS 140-2 Validated Cryptography” on page 8 for more details).

This means files and messages stored by MOVEit DMZ cannot be read or altered by a hacker, even if they gain Administrator rights to the underlying operating system. The security of data stored by MOVEit DMZ does not depend on the underlying OS always being secure. Insecure storage is one of the critical security flaws cited on the Open Web Application Security Project (OWASP) ‘Top Ten’ list, which states:

“Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection. The impact...can be devastating to the security of a website.”

The following are included amongst the most common storage mistakes cited on the 'Top Ten' list.

- Insecure storage of keys, certificates, and passwords.
- Poor sources of randomness.
- Poor choice of algorithm.

MOVEit DMZ can be used to eliminate these problems by providing Portals and Web applications with access to its production proven, FIPS 140-2 validated 256-bit AES encrypted secure storage services.

SECURE USER DATABASE SERVICES

MOVEit DMZ includes its own built-in, commercially licensed database, which it employs to securely store user information, including authentication information and permissions. Web applications can also make use of the MOVEit DMZ user database as a service.

OWASP recommends using SHA-1 hashing to protect passwords, and that is what MOVEit DMZ does using its FIPS 140-2 validated SHA-1 hash capability.

Commercial use of its user database is provided for under the MOVEit DMZ Basic license, which permits an unlimited number of users in the database (there is no per user fee).

EXTERNAL AUTHENTICATION

MOVEit DMZ has its own built-in secure database that it automatically authenticates users against, but it must be able to access the same authentication source that the application is using in order to authenticate a Portal or Web app user session when it is transferred or duplicated to MOVEit DMZ.

There are a number of different ways that MOVEit DMZ can do this.

This source can be MOVEit DMZ's own internal user database, if the Portal or Web app is using the MOVEit DMZ user database for authentication. MOVEit DMZ can also authenticate users against one or more ODBC-compliant databases that contain clear text usernames and passwords, and/or against any combination of the following LDAP, Secure LDAP and RADIUS Server accessible sources.

Active Directory (AD) by Microsoft via LDAP or Secure LDAP

Border Manager by Novell via RADIUS

eDirectory by Novell LDAP or Secure LDAP

Internet Authentication Services (IAS) by Microsoft via RADIUS

iPlanet by SUN via LDAP or Secure LDAP

Tivoli Access Manager by IBM via LDAP

MOVEit DMZ includes the following advanced capabilities for use with LDAP accessible servers.

User Replication. User properties, such as their email addresses and full names, can be looked up on an LDAP server by MOVEit DMZ and replicated during automatic user creation, user signon, and overnight scheduled processes.

Group Replication. Users belonging only to certain LDAP groups can be replicated, enabling MOVEit DMZ to bind to entire organizations, but only permit access for a subset of users, even across organizational units.

Custom Mapping. Administrators can use a macro syntax to map the specific properties of their LDAP user records to various fields on a MOVEit DMZ user profile.

User Expiration. MOVEit DMZ can automatically expire users in its user database who are no longer visible in the LDAP server(s) it is configured to authenticate against.

Configuration Testing. Step-by-step testing capabilities are built into MOVEit DMZ to assist administrators to correctly setup its LDAP and/or RADIUS configurations.

SiteMinder SSO Integration. Enables “single sign-on” to the MOVEit DMZ web interface for end-users who have authenticated through a CA eTrust SiteMinder portal authentication server.

While these External Authentication capabilities are an integral part of the MOVEit DMZ codebase, they are a separately licensed and priced option. Commercial use of this option requires a MOVEit DMZ Basic license with the External Authentication option enabled.

USER INTERFACE CUSTOMIZATION

MOVEit DMZ includes a wide range of features that can be used to customize and control its Web user interface to make it look and feel like part of a specific application.

MOVEit DMZ’s Web end user interface uses cascading style sheets (CSS). Administrators can use the product’s stock color schemes, or implement their own custom scheme, to control font types, sizes and colors as well as background colors and images. Custom HTML banners (with Flash logos and/or JavaScript menus if desired) can be used, and custom Help files can also be implemented.

MOVEit DMZ Administrators can even select which MOVEit DMZ functions are visible to/usable by specific users, or groups of users, and can even suppress all of the native MOVEit DMZ Web end-user navigation in order to substitute a custom navigation system of their choice.

MULTI-LINGUAL END-USER INTERFACE

This option enables each MOVEit DMZ user or group of users to select the English, French or Spanish language Web end-user interface for file transfers, secure messaging, receiving file and message arrival email notifications, and accessing Help. These language interfaces are an integral part of the MOVEit DMZ codebase, but French and Spanish are each licensed and priced as separate options.

HIGH AVAILABILITY OPTION

MOVEit DMZ has a well earned a reputation as a stable product, but it can be deployed to provide failover and scalability when deployed on two or more load-balanced production host systems in conjunction with either a local network-attached storage (NAS) or a storage area network (SAN) that can be accessed as a NAS. MOVEit DMZ high availability requires a minimum of two identical MOVEit DMZ commercial licenses (there are no separate licensing or maintenance fees for this).

FIPS 140-2 VALIDATED CRYPTOGRAPHY

Another unique MOVEit DMZ feature is its fully integrated Federal Information Processing Standards (FIPS) 140-2 validated cryptographic software module. Ipswitch developed this module, which was one of the very first to achieve FIPS 140-2 validation. It includes the following functions.

256-bit AES Encryption. This is used to safeguard each and every file and message received by MOVEit DMZ, including those generated or used by Web applications.

SHA-1 Hashing. This is used to safeguard administrative and user passwords.

Pseudo-Random Number Generator. This is used to generate certain random identifiers, such as file IDs, folder IDs, and message keys.

Achieving FIPS validation takes considerable time and money. An independent testing lab approved by the US and Canadian governments must inspect the module’s design documents, source code and related materials, and subjects the software to extensive testing designed to confirm the following.

All approved algorithms in the module are securely implemented
There are no hidden “back doors” into the module
Sensitive data is securely erased by the product when not needed

Since adding it in 2003, MOVEit DMZ has been one of the very few secure transfer products that has included its own built-in FIPS 140-2 validated cryptography. Commercial use of these capabilities is provided for under the MOVEit DMZ Basic license (see below for details).

MOVEIT DMZ LICENSING

The MOVEit DMZ Basic software is licensed for installation on a single production system, and also on a single non-production system (additional non-production systems can be added to the license). The systems can be physical or virtual, and the type and number of available CPU's does not matter. In addition, the MOVEit DMZ Basic license permits all of the following.

An unlimited number of users

An unlimited number of transfers

An unlimited number of files (and messages if licensed) stored on the server

Acquisition of the Basic license involves paying a one-time fee and an annual maintenance fee.

The MOVEit DMZ API is a separately priced option that provides unlimited use of the API interface and the MOVEit DMZ API Java class, Windows COM component, and their command-line interfaces. Acquisition of this option involves paying a one-time API license fee and an annual maintenance fee.

Secure Messaging is a separately priced option that provides the right for an unlimited number of users to create, send, store and receive an unlimited number of messages (with or without files). When used with the API this option also allows unlimited use of Secure Messaging by applications.

This option involves paying a one-time Secure Messaging license fee and an annual maintenance fee.

MOVEIT DMZ EVALUATION OPTIONS

There are two ways to evaluate MOVEit DMZ and the MOVEit API with a portal or Web application. Both options will allow you to evaluate complete commercial copies of these software products, and both will enable you to do the following with a Web browser or MOVEit DMZ API client.

Add and modify MOVEit DMZ users, groups, folders and permissions

Transfers files, with or without optional email file arrival notifications

Create and exchange messages, with or without attached files

Examine the MOVEit DMZ audit trail on a per user, file or message basis

Alter the MOVEit DMZ user interface branding (color scheme, logos, etc.)

Change which MOVEit DMZ functions and features users can see and use

Both options typically run for 30 days, include tech support from Standard Networks, and are free.

Online Evaluation. This option involves setting up an evaluation account on an Internet accessible MOVEit DMZ server managed by Ipswitch. Set up includes branding MOVEit DMZ for your portal or Web application, and providing the evaluator with administrative control of the account. We provide the software and host, and do the set up work (typically in one day).

We typically recommend trying MOVEit DMZ online first because it is usually the fastest way for you to determine if the product will meet your requirements. If you later wish to do an onsite evaluation, then Ipswitch will be happy to make arrangements for one of these too, without charge.

Onsite Evaluation. Under this option Ipswitch provides the evaluator with permission to download the MOVEit DMZ software, and a limited term license key to activate it. The evaluator provides a suitable Windows 2003 system, and the necessary time and expertise to install and configure MOVEit DMZ within their hardware/software/security environment. This provides the very best opportunity to fully evaluate the product, and it will take less than one minute to enter your commercial license key to enable it for production use if your organization purchases a license. Onsite evaluations also enable testing of the MOVEit DMZ External Authentication capabilities.

For additional information, please contact the Ipswitch File Transfer division or visit www.IpswitchFT.com.



Contact Ipswitch's File Transfer Division